R E P U B L I Q U E  F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 03 JUIL. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

## REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W / 010801

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 19 JUIL 2002
75 INPI PARIS
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 0209205
DATE DE DÉPÔT ATTRIBUÉE
PAR L'INPI 19 JUIL. 2002

**Vos références pour ce dossier** *(facultatif)* JMD/NC/BFE020171

**1** NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

**CABINET PLASSERAUD**

84, rue d'Amsterdam
75440 PARIS CEDEX 09

**Confirmation d'un dépôt par télécopie** ☐ N° attribué par l'INPI à la télécopie

**2 NATURE DE LA DEMANDE** — **Cochez l'une des 4 cases suivantes**

| | | |
|---|---|---|
| Demande de brevet | ☒ | |
| Demande de certificat d'utilité | ☐ | |
| Demande divisionnaire | ☐ | |
| *Demande de brevet initiale* | N° | Date |
| *ou demande de certificat d'utilité initiale* | N° | Date |
| Transformation d'une demande de brevet européen *Demande de brevet initiale* | ☐ N° | Date |

**3 TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE D'ENREGISTREMENT DANS UNE CARTE A PUCE ET CARTE A PUCE POUR METTRE EN OEUVRE CE PROCEDE

**4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE**

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

**5 DEMANDEUR** (Cochez l'une des 2 cases) ☐ **Personne morale** ☐ **Personne physique**

| | | |
|---|---|---|
| Nom ou dénomination sociale | | GROUPEMENT DES CARTES BANCAIRES |
| Prénoms | | |
| Forme juridique | | GROUPEMENT D'INTERET ECONOMIQUE |
| N° SIREN | | 3 3 13 02 79 4 |
| Code APE-NAF | | |
| Domicile ou siège | Rue | 31 rue de Berri |
| | Code postal et ville | 7 5 0 0 8 PARIS |
| | Pays | FRANCE |
| Nationalité | | Française |
| N° de téléphone *(facultatif)* | | N° de télécopie *(facultatif)* |
| Adresse électronique *(facultatif)* | | |

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

Procédé d'enregistrement dans une carte à puce et carte à puce pour mettre en œuvre ce procédé.

Le domaine de l'invention est celui des transactions validées par une communication entre un terminal et un microcircuit protégé.

On connaît par exemple les cartes à microcircuit ou cartes à puce dans lesquelles le microcircuit comprend un microprocesseur et une mémoire interne.

La mémoire interne de chaque carte contient des moyens de reconnaissance d'un code secret propre à la carte de façon à ne valider une transaction que lorsque le détenteur de la carte communique un code qui correspond au code secret. Le microcircuit étant protégé contre les intrusions, une validation de transaction par la carte, est reconnue constituer une preuve selon laquelle le détenteur légitime de la carte, a accepté la transaction.

L'état connu de la technique divulgue de nombreux moyens de sécurisation du microcircuit, du terminal et des communications entre le microcircuit et le terminal, tels que les procédés cryptographiques, les destructions sur tentative d'effraction.

Cependant, le détenteur légitime de la carte peut être tenté de réfuter la preuve en prétextant par exemple qu'un dysfonctionnement du terminal ou des moyens de communication avec le terminal, ou encore qu'une

- le microprocesseur émet un signal de validation de transaction vers l'extérieur de la carte, après avoir enregistré le cryptogramme dans la mémoire interne.

L'enregistrement dans la mémoire interne, du cryptogramme sur les données de la transaction, constitue un élément matériel et donc tangible de preuve que la transaction sur les données de laquelle porte le cryptogramme, a été réalisée à l'aide de la carte. Si le détenteur légitime de la carte tente de répudier la transaction, il est alors possible d'ordonner une lecture de la mémoire interne pour mettre en évidence le cryptogramme.

L'émission du signal de validation après avoir enregistré le cryptogramme, évite qu'une transaction soit validée sans que le cryptogramme ne soit enregistré. Si le détenteur de la carte retire celle-ci du lecteur qui l'alimente en puissance pour en arrêter le fonctionnement, le retrait de la carte immédiatement après l'émission du signal de validation, ne peut pas empêcher que le cryptogramme soit enregistré.

Le fait que l'enregistrement dans la mémoire interne soit effectué par le microprocesseur de la carte dès qu'il détecte un événement conforme, empêche un élément extérieur d'imposer un enregistrement falsifié dans la carte.

Un deuxième objet de l'invention, est une carte à microcircuit comprenant un microprocesseur et une mémoire

Le nombre de bornes n'est pas limitatif. On sait par exemple que de nombreuses cartes possèdent huit bornes plates.

Le microcircuit 2 comprend un microprocesseur 15 et une mémoire interne 16. Un bus interne 17 permet au microprocesseur 15 de traiter des données numériques reçues par des moyens de réception 14 connectés à la borne plate 7, des données numériques à émettre par des moyens d'émission 12 connectés à la borne plate 4, à l'aide de données numériques contenues dans la mémoire 16.

Des moyens d'alimentation 13 connectés aux bornes plates 5 et 6, sont agencés pour alimenter électriquement le microprocesseur 15, la mémoire interne 16, les moyens de réception 14 et les moyens d'émission 12. La mémoire interne 16 est telle qu'elle conserve ses données en absence d'alimentation électrique.

Le lecteur 3 comprend de façon connue un clavier 18 et un écran 19.

Pour effectuer une transaction, la carte 1 est introduite dans le lecteur 3 de façon à mettre en contact électrique chacune des bornes 4, 5, 6, 7 avec respectivement chacune des bornes 8, 9, 10, 11.

Les bornes 9 et 10 fournissent l'alimentation électrique de la carte 1. La borne 8 permet au lecteur 3 de recevoir les données numériques émises par la carte 1.

comprenant par exemple une date (année, mois, jour, heure, minutes) et un montant monétaire.

Si un litige ultérieur intervient sur la transaction, une lecture du cryptogramme dans le microcircuit permet de prouver que le cryptogramme correspond effectivement à cette transaction.

L'intégralité des données pourrait être enregistrée. Cependant le cryptogramme offre l'avantage d'un enregistrement plus compact qui utilise moins de place en mémoire interne tout en offrant les garanties de sécurité suffisantes obtenues par des fonctions cryptographiques, par exemple des fonctions de hachage connues ou de chiffrement à la clé publique.

Le cryptogramme est amélioré lorsqu'il porte aussi sur les données de transaction qui comprennent un identificateur de destinataire de la transaction. Ceci permet d'assurer que la transaction n'a pas été détournée.

La fiabilité de l'enregistrement est renforcée par le fait que c'est le processeur 15 lui-même qui génère l'événement conforme de la transition 21 et non pas un équipement extérieur tel que le lecteur 3 ou tout autre terminal.

Avantageusement, l'événement conforme résulte d'une comparaison effectuée par le microprocesseur 15 dans une étape 23. L'étape 23 est activée à partir de l'étape 20,

Revendications:

1. Procédé pour générer un élément tangible de preuve qui garantit qu'une transaction déterminée a été réalisée en utilisant une carte (1) à microcircuit déterminée, le microcircuit (2) de ladite carte comprenant un microprocesseur (15) et une mémoire interne (16), caractérisé en ce qu'il comprend des étapes (22,27) dans lesquelles:

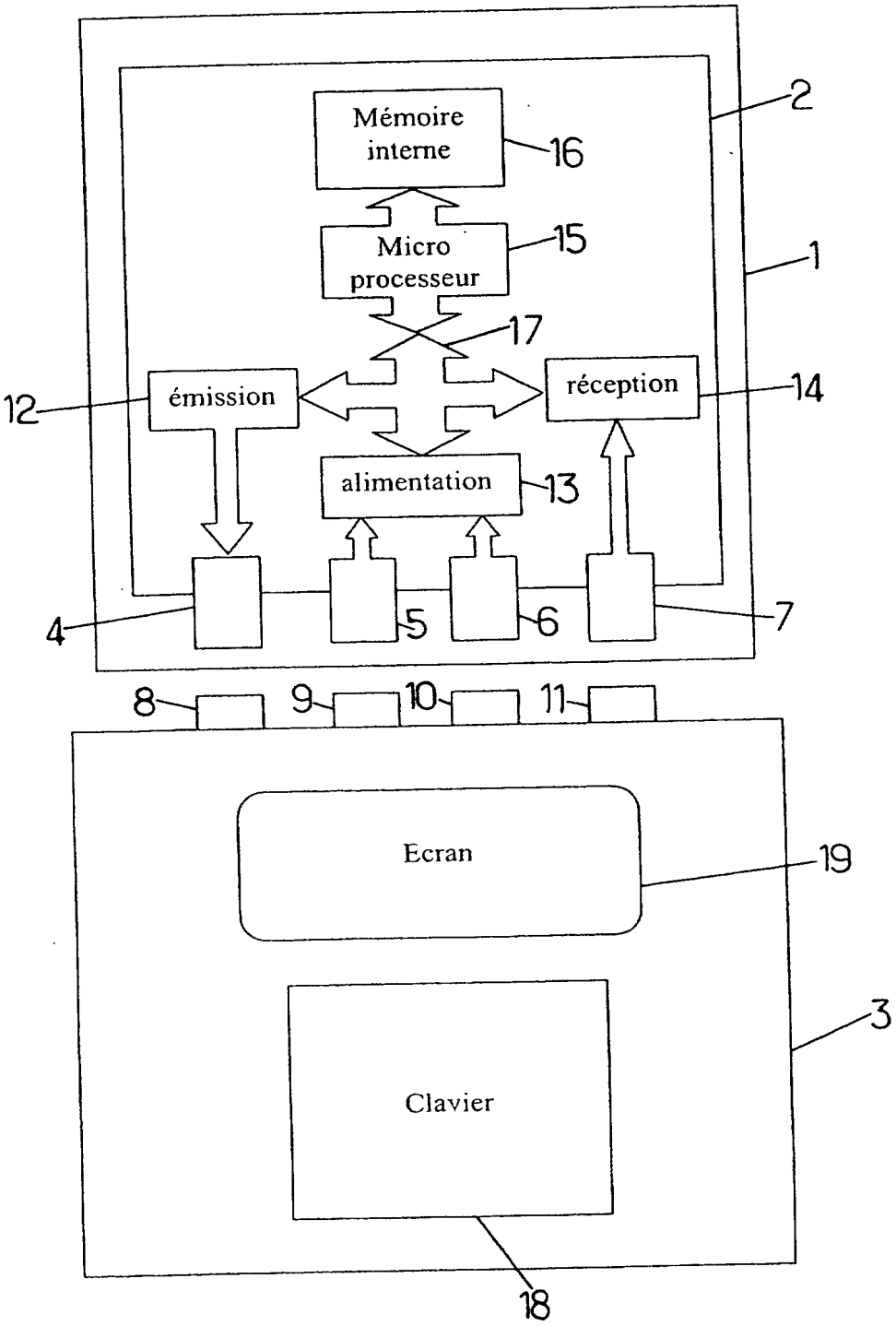
- le microprocesseur enregistre dans la mémoire interne, un cryptogramme sur les données de la transaction, dès qu'il détecte un événement conforme pour valider la transaction,
- le microprocesseur émet un signal de validation de transaction vers l'extérieur de la carte, après avoir enregistré le cryptogramme dans la mémoire interne.

2. Procédé selon la revendication 1, caractérisé en ce que ledit événement conforme résulte d'une comparaison effectuée par le microprocesseur qui vérifie qu'un code reçu est égal à un code secret détenu dans la mémoire interne.

3. Procédé selon la revendication 1, caractérisé en ce que les données de la transaction comprennent une date et un montant monétaire.

4. Procédé selon la revendication 3, caractérisé en ce que les données de la transaction comprennent un identificateur de destinataire de la transaction.

FIG.1.


Mémoire interne
16
2
Micro processeur
15
1
17
émission
12
réception
14
alimentation
13
4
5
6
7
8
9
10
11
Ecran
19
3
Clavier
18

reçue le 12/08/02

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

# BREVET D'INVENTION
## CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

## DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 270601

| | |
|---|---|
| **V s références pour ce dossier** *(facultatif)* | JMD/NC/BFF020171 |
| **N° D'ENREGISTREMENT NATIONAL** | 02 09 205 |

**TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE D'ENREGISTREMENT DANS UNE CARTE A PUCE ET CARTE A PUCE POUR METTRE EN OEUVRE CE PROCEDE

**LE(S) DEMANDEUR(S) :**

GROUPEMENT DES CARTES BANCAIRES

**DESIGNE(NT) EN TANT QU'INVENTEUR(S) :**

| | | |
|---|---|---|
| **1** Nom | | |
| Prénoms | | ANDRAUD Sylvie |
| Adresse | Rue | 42 rue d'Artois |
| | Code postal et ville | 75008 PARIS FRANCE |
| Société d'appartenance *(facultatif)* | | |
| **2** Nom | | |
| Prénoms | | ZWAENEPOEL Evelyne |
| Adresse | Rue | 6, avenue Benoit Levy |
| | Code postal et ville | 94160 Saint-Mandé FRANCE |
| Société d'appartenance *(facultatif)* | | |
| **3** Nom | | |
| Prénoms | | MEGGLE Claude |
| Adresse | Rue | 104 Bd Arago |
| | Code postal et ville | 75014 PARIS FRANCE |
| Société d'appartenance *(facultatif)* | | |

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

**DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)**

Le 19 juillet 2002

**CABINET PLASSERAUD**

Jean Marc DIOU

CPI N° 00-1001